BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

[redacted]

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/764,844	01/17/2001	Ronald P. Doyle	RSW920010007US1	6508

7590 08/02/2004

Jeanine S. Ray-Yarletts
IBM Corporation T81/503
PO Box 12195
Research Triangle Park, NC 27709

EXAMINER	
COLIN, CARL G	
ART UNIT	**PAPER NUMBER**
2136	

DATE MAILED: 08/02/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/764,844	DOYLE ET AL.	
	Examiner	Art Unit	
	Carl Colin	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 January 2001* .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-78* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-78* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *17 January 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) *2/15/02* .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other:

DETAILED ACTION

1. Pursuant to USC 131, claims 1-78 are presented for examination.

Specification

2. The disclosure is objected to because of the following informalities: on page 1, the related patent applications have no serial numbers. Applicant is required to add the following patent numbers: on page 8, line 8 US Patent "6772331", Appropriate correction is required.

2.1 The lengthy specification has not been checked to the extent necessary to determine the presence of all possible minor errors. Applicant's cooperation is requested in correcting any errors of which applicant may become aware in the specification.

2.2 The abstract of the disclosure is objected to because it contains the term "the disclosed techniques". Correction is required. See MPEP § 608.01(b).

Applicant is reminded of the proper language and format for an abstract of the disclosure.

The abstract should be in narrative form and generally limited to a single paragraph on a separate sheet within the range of 50 to 150 words. It is important that the abstract not exceed 150 words in length since the space provided for the abstract on the computer tape used by the printer is limited. The form and legal phraseology often used in patent claims, such as "means" and "said," should be avoided. The abstract should describe the disclosure sufficiently to assist readers in deciding whether there is a need for consulting the full patent text for details.

The language should be clear and concise and should not repeat information given in the title. It should avoid using phrases which can be implied, such as, "The disclosure concerns," "The disclosure defined by this invention," "The disclosure describes," etc.

2.3 The disclosure is objected to because it contains embedded hyperlinks and/or other form of browser-executable codes (see page 4, line 16; and page 29, line 7). Applicant is required to delete the embedded hyperlinks and/or other form of browser-executable codes. See MPEP § 608.01.

2.4 The use of the trademark "WORKPAD" and "PALMPILOT" has been noted in this application, for instance on page 2, lines 16-18. It should be capitalized wherever it appears and be accompanied by the generic terminology.

Although the use of trademarks is permissible in patent applications, the proprietary nature of the marks should be respected and every effort made to prevent their use in any manner which might adversely affect their validity as trademarks.

Claim Objections

3. **Claims 10, 42, and 65**, are objected to because of the following informalities: on lines 2 and 3, "hardware reset of the component" and operably connecting of the component needs to be revised. There is lack of antecedent basis for these claims . Appropriate correction is required.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an

> international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

4.1 **Claims 1-4, 6, 7, 10, 13, 14, 16, 17, 19, 33-36, 38, 39, 42, 45, 46, 48, 49, 51, 56-59, 61, 62, 65, 68, 69, 71, 72, and 74** are rejected under 35 U.S.C. 102(e) as being anticipated by US Patent 6,125,192 to **Bjorn et al.**.

4.2 **As per claims 1, 14, 33, 46, 56, and 69, Bjorn et al.** discloses a system for securely providing biometric input from a user, comprising: a biometric sensor, a security component which provides security functions, such that the security component can vouch for authenticity of components with which it is securely operably connected, for example (see column 4, line 39 through column 5, line 22; see also column 5, line 43 through column 6, line 27); a card containing stored secrets and stored identifying information pertaining to an authorized holder of the card, for example (see column 4, line 39 through column 5, line 22 and column 6, lines 18-27); a card reader for accessing the stored secrets and stored identifying information, for example (see column 4, line 39 through column 5, line 22); means for operably inserting the card into the

card reader, for example (see column 16, lines 33-43); and means for securely operably connecting the biometric sensor, the card reader, and the security component, for example (see column 4, line 39 through column 5, line 22; see also column 5, line 43 through column 6, line 27 and column 4, line 39 through column 5, line 22).

As per claims 2, 16, 34, 48, 57, and 71, Bjorn et al discloses the limitation of wherein the stored identifying information comprises stored biometric information of the authorized holder, and further comprising means for comparing biometric information obtained with the biometnc sensor from a user of the system, to the stored biometric information of the authorized holder, **Bjorn et al** also discloses wherein the means for comparing is performed by the biometric sensor, for example (see column 6, lines 27-43).

As per claims 3, 35, and 58, Bjorn et al. discloses the limitation of wherein selected ones of the secure operable connections are made using one or more buses of the security component, for example (see column 4, line 39 through column 5, line 22).

As per claims 4, 36, and 59, Bjorn et al. discloses the limitation of wherein selected ones of the operable connections are made using a wireless connection between respective ones of the components and the security component, for example (see column 4, lines 18-22).

As per claims 6, 38, and 61, Bjorn et al. discloses the limitation of wherein selected ones of the secure operable connections are provided when the security component is manufactured, for example (see column 9, lines 52-62).

As per claims 7, 39, and 62, Bjorn et al. discloses the limitation of wherein the components comprise one or more of (1) input/output components and (2) application processing components, for example (see column 8, lines 4-30).

As per claims 10, 42, and 65, Bjorn et al. discloses the limitation of wherein the means for securely operably connecting is activated by a hardware reset of the component, and wherein the hardware reset is activated by operably connecting of the component, for example (see column 8, lines 4-30).

As per claims 13, 45, and 68, Bjorn et al. discloses the limitation of further comprising means for concluding that the user is the authorized holder of the card only if the means for comparing succeeds, for example (see column 6, lines 27-43 and column 16, line 50 through column 17, line 5).

As per claims 17, 49, and 72, Bjorn et al. discloses the limitation of further comprising means for securely transferring the stored biometric information of the authorized holder to the biometric sensor for use by the means for comparing, for example (see column 6, lines 28-43 and column 17, lines 50-67).

As per claims 19, 51, and 74, Bjorn et al. discloses the limitation of wherein the means for comparing is performed by the security component, for example (see column 8, line 60 through column 9, line 3).

5. **Claims 24-32** are rejected under 35 U.S.C. 102(e) as being anticipated by US Patent 6,325,285 to **Baratelli**.

5.1 **As per claim 24, Baratelli** discloses a card which contains one or more previously-stored secrets of an authorized holder of the card and which has a biometric sensor embedded on a surface thereof, for example (see abstract).

As per claim 25, Baratelli discloses the limitation of wherein the biometric sensor is a fingerprint sensor, and wherein the previously-stored secrets include a fingerprint of the authorized card holder, for example (see column 7, lines 5-27 and abstract).

As per claim 26, Baratelli discloses the limitation of wherein the biometric sensor is a palm,print sensor, and wherein the previously-stored secrets include a palm print of the authorized card holder, for example (see column , lines).

As per claim 27, Baratelli discloses the limitation of wherein the biometric sensor is a voice print sensor, and wherein the previously-stored secrets include a voice print of the authorized card holder, for example (see column 9, lines 45-67).

As per claim 28, Baratelli discloses the limitation of wherein the biometric sensor is a retina scanner, and wherein the previously-stored secrets include a retina scan of the authorized card holder, for example (see column 9, lines 45-67).

As per claim 29, Baratelli discloses the limitation of wherein the biometric sensor is a skin chemistry sensor, and wherein the previously-stored secrets include a skin chemistry of the authorized card holder, for example (see column 9, lines 38-67).

As per claim 30, Baratelli discloses the limitation of wherein the previously-stored secrets include stored biometric information of the authorized holder, and further comprising means for comparing biometric information that is obtained with the biometric sensor from a user, to the stored biometric information of the authorized holder, for example (see column 7, lines 5-27 and abstract).

As per claim 31, Baratelli discloses the limitation of further comprising means for accessing selected ones of the previously-stored secrets only if the means for comparing determines that the obtained biometric information of the user matches the stored biometric information of the authorized holder, for example (see column 7, lines 5-27).

As per claim 32, Baratelli discloses the limitation of wherein the previously-stored-secrets include a private cryptographic key of the authorized holder, and wherein the means for accessing further comprising means for accessing the private key to compute a digital signature over information presented to the card, for example (see column 7, lines 27-45).

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6.1 **Claims 5, 8, 9, 11, 12, 15, 18, 20, 21, 22, 23, 37, 40, 41, 43, 44, 47, 50, 52, 53, 54, 55, 60, 63, 64, 66, 67, 70, 73, 75, 76, 77, and 78** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 6,125,192 to **Bjorn et al.** in view of US Patent 6,330,670 to **England et al.**.

6.2 **As per claims 5, 22, 37, 54, 60, and 77, Bjorn et al.** substantially teaches a method and system for securely providing biometric input from a user and means for securely operably connecting the biometric sensor the digital system that meets the recitation of the security component and the receiving unit that meets the recitation of the card reader. **Bjorn et al.** discloses an embodiment using a network, for example (see figure 3) and also discloses the sensor can be connected to a wireless system, or any indirect digital connection, for example (see column 4, lines 18-22). **Bjorn et al.** further discloses mutual authentication using public/private key and using a key each time a session is established and a timestamp to prevent stealing of the key, for example (see column 10, lines 1-22). It is very well known in the art wireless connection using SSL data encryption or equivalent that provides mutual authentication of both endpoints with a limited one-time key. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the system of **Bjorn et al.** to provide wireless connections use Secure Sockets Layer (SSL) data encryption or an equivalent which provides mutual authentication of both endpoints, negotiation of a time-limited key agreement with secure passage of a selected encryption key, and periodic renegotiation of the time-limited key agreement with a new encryption key as suggested by **Bjorn et al.** to prevent stealing of the key.

England et al. in an analogous art teaches secure communication between components using SSL whereas keys are valid for a short period of time to prevent the key from being compromised, for example (see column 15, lines 29-45 and column 20, lines 40-57). **England et al.** also discloses a unique device identifier that is used to identify data originating therefrom, a digital certificate, a private cryptographic key and a public cryptographic key that is

cryptographically-associated with the private cryptographic key, for example (see column 12, lines 53-65). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the system of **Bjorn et al.** to provide wireless connections use Secure Sockets Layer (SSL) data encryption or an equivalent which provides mutual authentication of both endpoints, negotiation of a time-limited key agreement with secure passage of a selected encryption key, and periodic renegotiation of the time-limited key agreement with a new encryption key as taught by **England et al.**. This modification would have been obvious because one skilled in the art would have been motivated by the suggestions provided by **England et al.** so as to prevent the key from being compromised.

As per claims 8, 9, 11, 12, 21, 40, 41, 43, 44, 53, 63, 64, 66, 67, and 76, Bjorn et al. discloses the limitation of wherein the means for securely operably connecting further comprises means for authenticating the biometric sensor to the security component and means for authenticating the security component to the biometric sensor, for example (see column 9, line 30 through column 10, line 7) and security handshake, for example (column 6, lines 52-65). **Bjorn et al.** discloses the limitation of wherein the means for authenticating the biometric sensor securely stored thereon. **Bjorn et al.** is silent about authenticating the card reader because of using an integral reader in its preferred embodiment, however, **Bjorn et al.** also discloses using a reader that can be attached to the security component through any connection, for example (see column 4, line 65 through column 5, line 6); when using an integral component, no duplicative memory, security units would be required otherwise strict security is necessary, for example (see column 5, lines 45-65). Therefore, one skilled in the art would be able to use disclosed by **Bjorn**

et al. with a separate reader that will require the same authentication as the one for the sensor. It is apparent apparent to one skilled in the art that one can mutually authenticate the card reader with the security component without departing from the scope and the spirit of the invention disclosed by **Bjorn et al.**.

England et al. in an analogous art also teaches mutual authentication of more than one component, for example (see column 12, lines 53-65) to provide a tamper resistant system. Therefore these claims are rejected on the same rationale as the rejection of claims 5, 37, and 60 above.

As per claims 15, 18, 47, 50, 70, and 73, Bjorn et al. discloses the limitation of wherein the stored secrets comprise a private key and a public key which are cryptographically related using public key cryptography, and further comprising means for digitally signing information presented to the card with the private key if the means for comparing succeeds and if the biometric sensor, the card reader, and the security component remain securely operably connected, for example (see column 4, line 65 through column 5, line 6 and column 16, lines 32-67). The authentication of the card reader was discussed above. Therefore these claims are rejected on the same rationale as the rejection of claims 5, 37, and 60. **Bjorn et al.** discloses a cross-authentication that would not be possible if the component is removed from the system (as mentioned in column 7, US Patent 6,577,733).

As per claims 20, 52, and 75, Bjorn et al. discloses the limitation of further comprising means for securely operably connecting an application processing component to the security component, and wherein the information presented to the card is generated by the securely

operably connected application processing component, for example (see column 9, line 30 through column 10). **England et al.** also discloses application processing component to the security component to generate information from another component, for example (see column 12, lines 53-67). Therefore these claims are rejected on the same rationale as claims 5, 37, and 60.

Claims 23, 55, and 78 are similar to the rejected **claims 22, 54, and 77** except for incorporating the claimed method into a system. Therefore, **claims 23, 55, and 78** are rejected on the same rationale as the rejection of **claims 22, 54, and 77**.

Conclusion

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 703-305-0355. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Carl Colin
Patent Examiner
July 21, 2004

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100